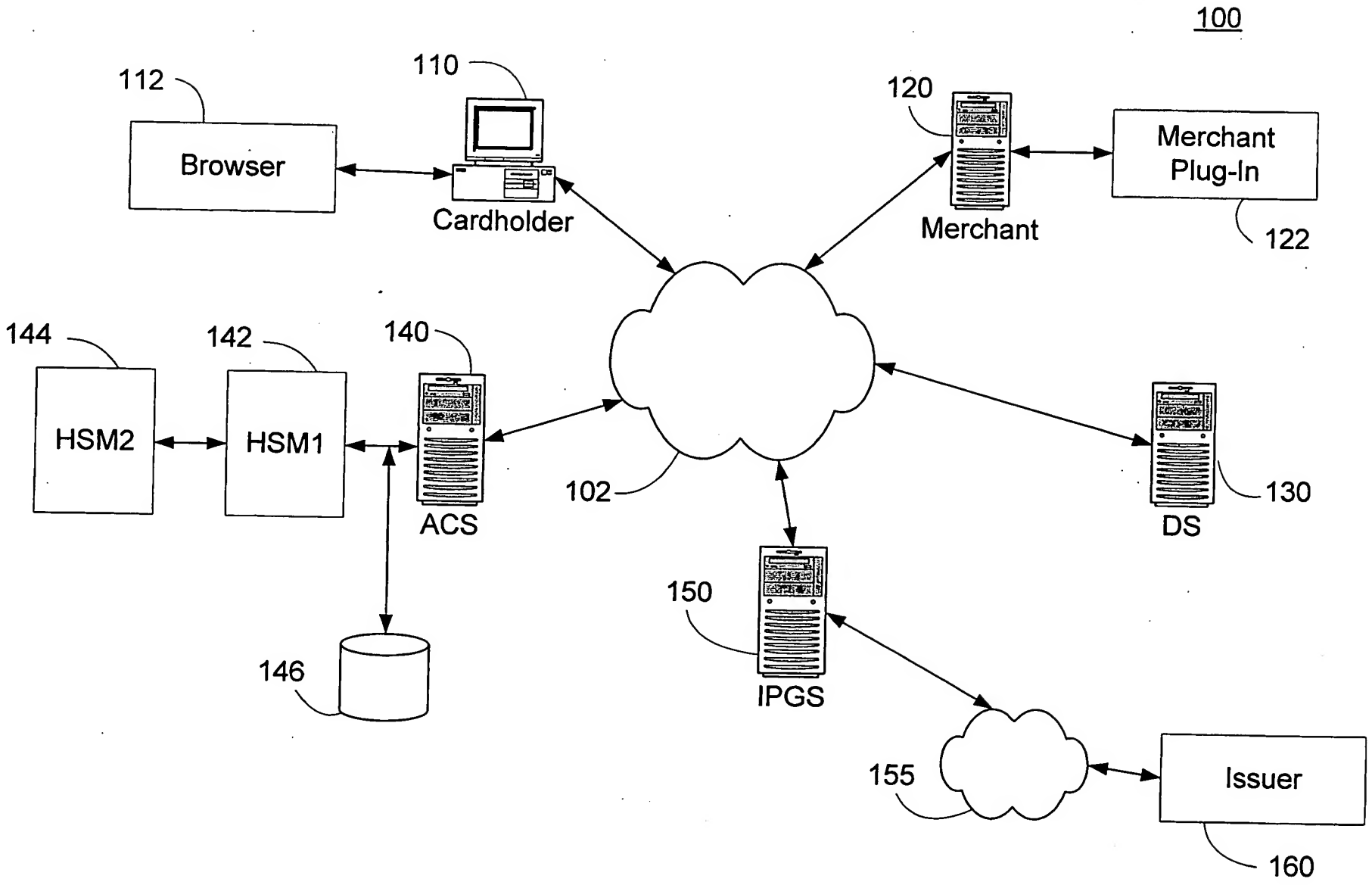
100
112
Browser
110
Cardholder
120
Merchant
Merchant Plug-In
122
144
HSM2
142
HSM1
140
ACS
102
130
DS
150
IPGS
146
155
Issuer
160

FIG. 1

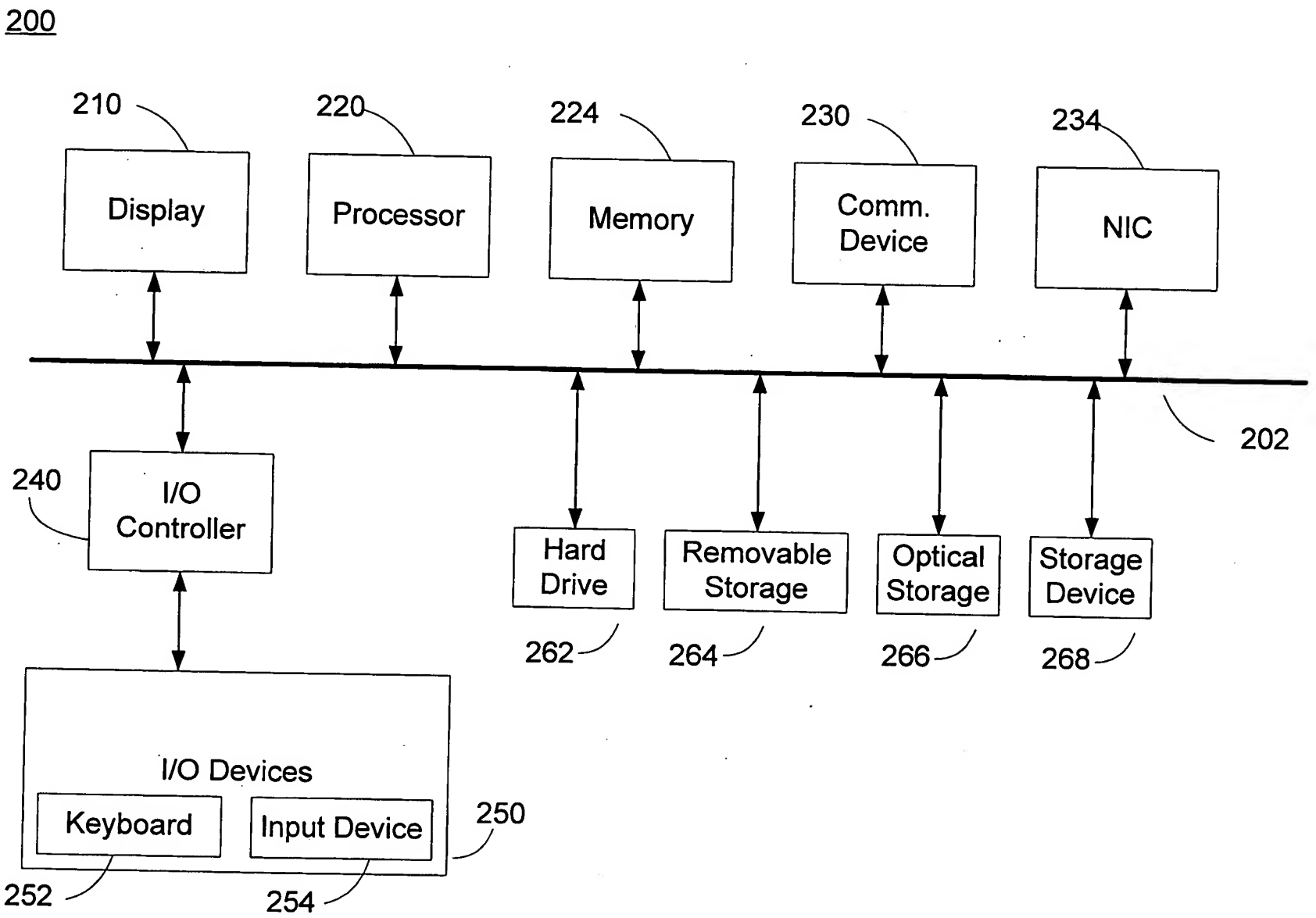
200
210
Display
220
Processor
224
Memory
230
Comm. Device
234
NIC
202
240
I/O Controller
Hard Drive
262
Removable Storage
264
Optical Storage
266
Storage Device
268
I/O Devices
Keyboard
Input Device
250
252
254

FIG. 2

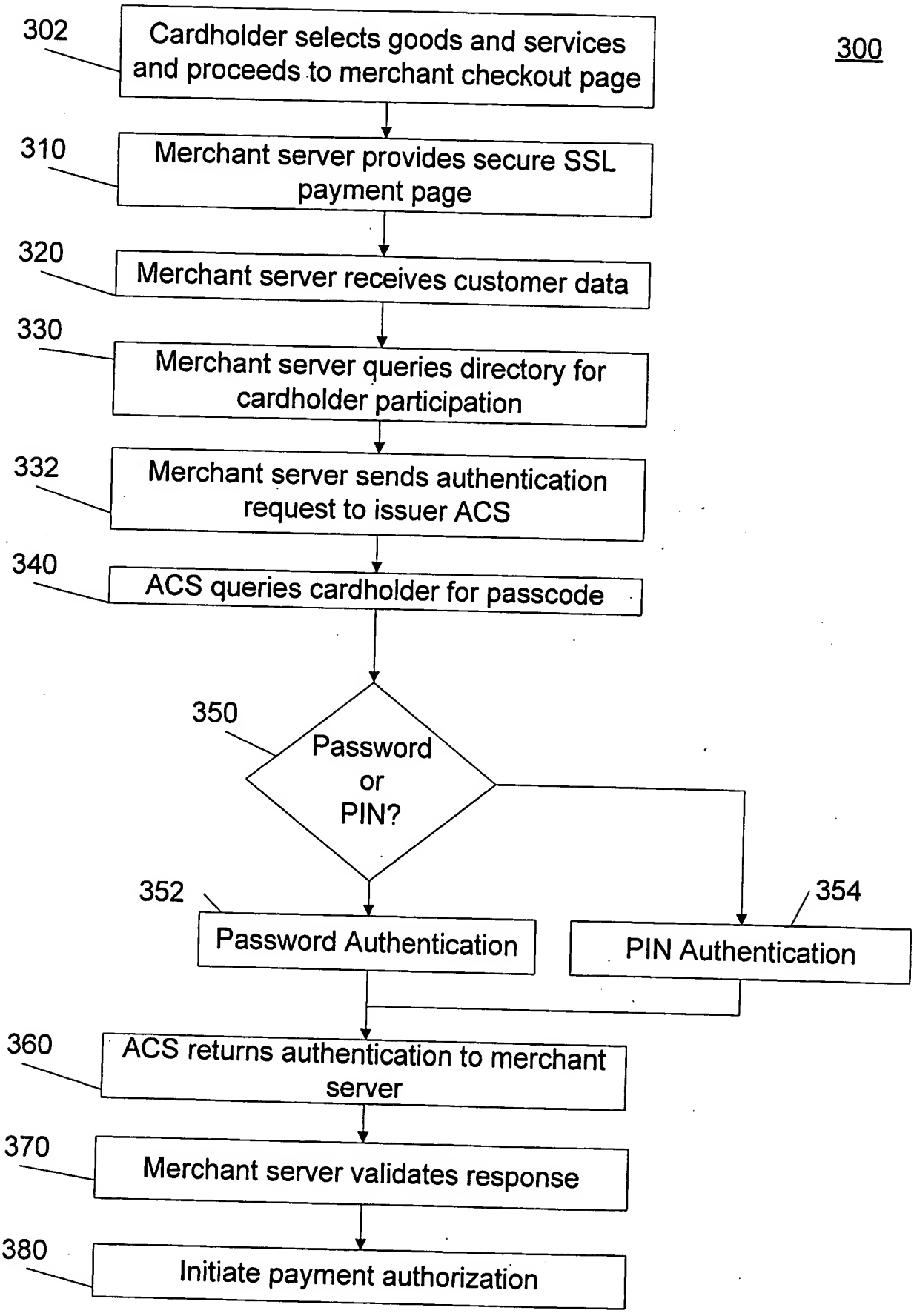
300
302
Cardholder selects goods and services and proceeds to merchant checkout page
310
Merchant server provides secure SSL payment page
320
Merchant server receives customer data
330
Merchant server queries directory for cardholder participation
332
Merchant server sends authentication request to issuer ACS
340
ACS queries cardholder for passcode
350
Password or PIN?
352
Password Authentication
354
PIN Authentication
360
ACS returns authentication to merchant server
370
Merchant server validates response
380
Initiate payment authorization

FIG. 3

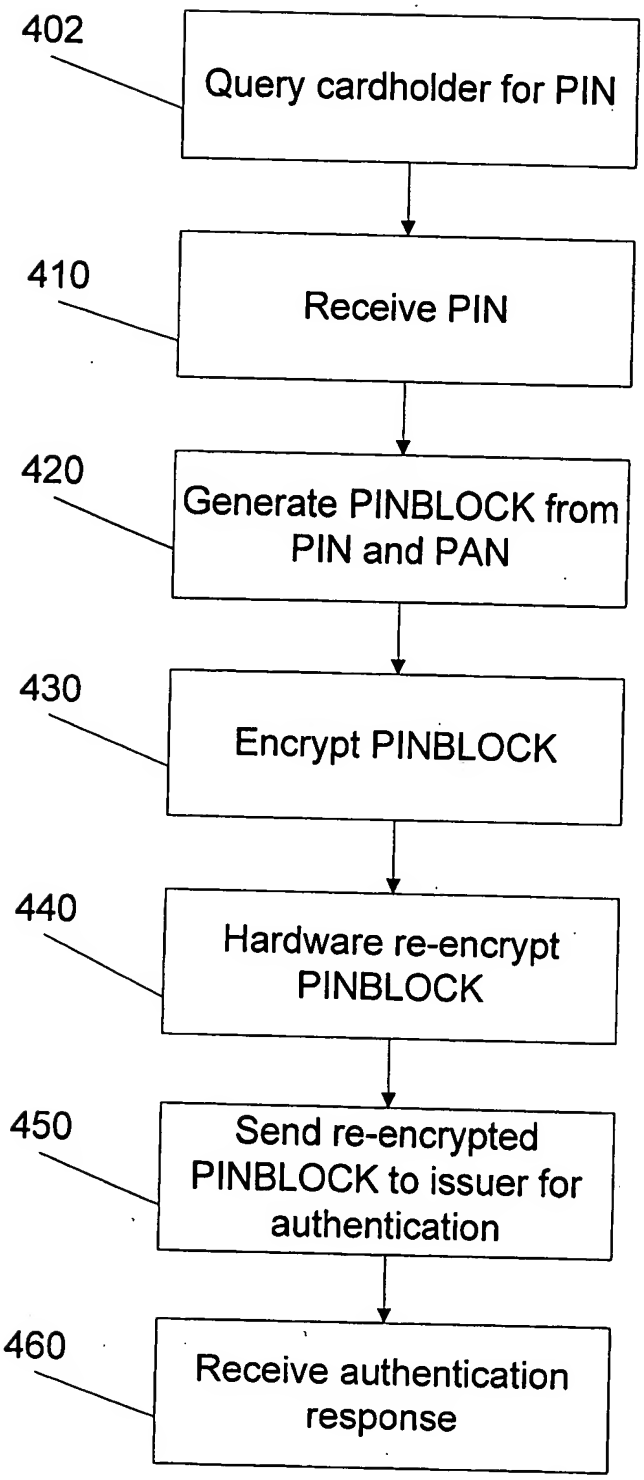
402
Query cardholder for PIN
410
Receive PIN
420
Generate PINBLOCK from PIN and PAN
430
Encrypt PINBLOCK
440
Hardware re-encrypt PINBLOCK
450
Send re-encrypted PINBLOCK to issuer for authentication
460
Receive authentication response

FIG. 4

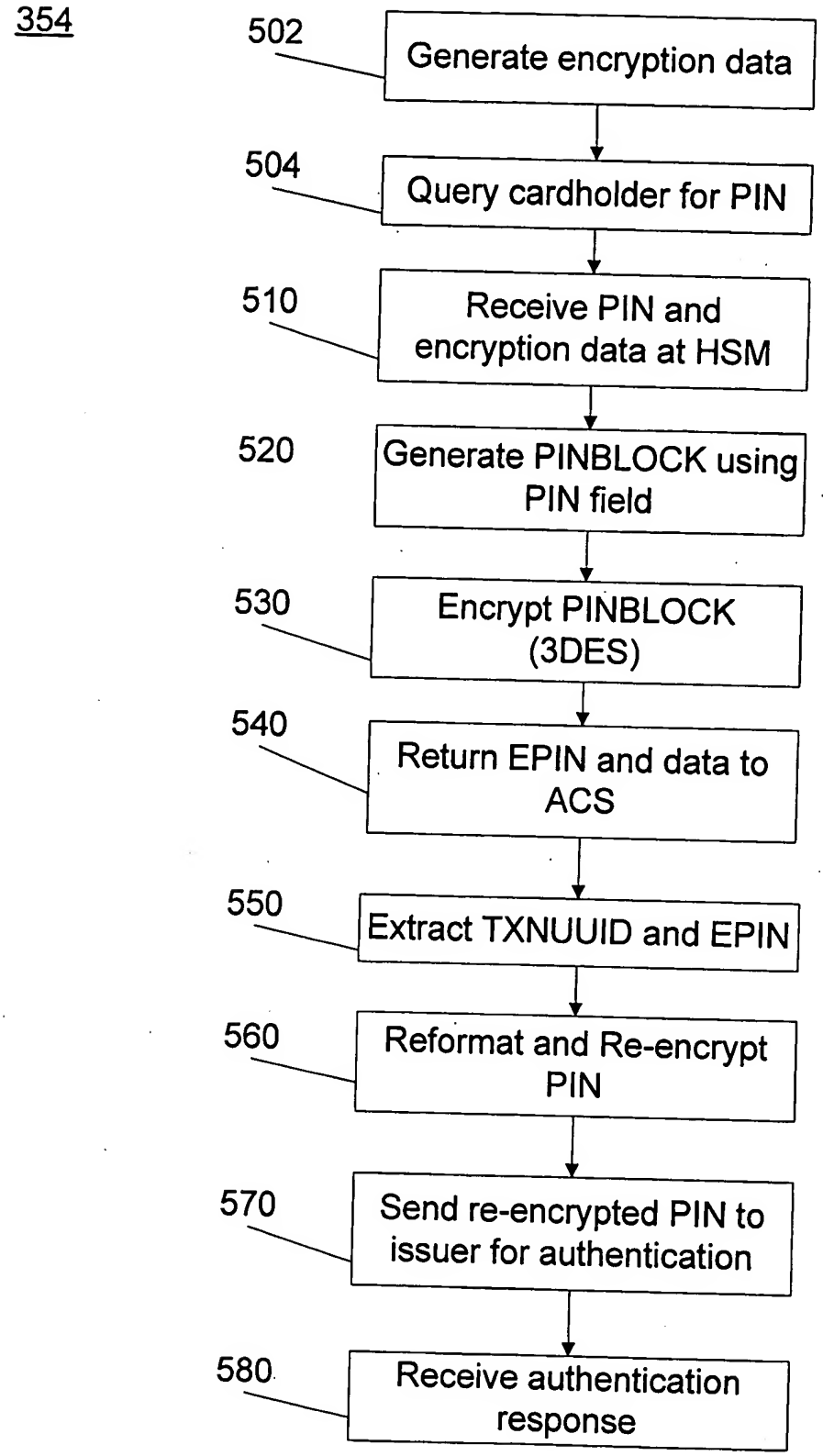
354
502
Generate encryption data
504
Query cardholder for PIN
510
Receive PIN and encryption data at HSM
520
Generate PINBLOCK using PIN field
530
Encrypt PINBLOCK (3DES)
540
Return EPIN and data to ACS
550
Extract TXNUUID and EPIN
560
Reformat and Re-encrypt PIN
570
Send re-encrypted PIN to issuer for authentication
580
Receive authentication response

FIG. 5

600

```
<html>
<head><title>PIN Entry Page</title></head>
<body>
<form method=POST name="PIN_Entry" action="https://www.acs-
      vbv.visa.com:9123/" autocomplete="off">
<p>Please enter your PIN:<p>
<table>
<tr><td>PIN:</td><td><INPUT TYPE="PASSWORD" name="pin"></td></tr>
</table>
<INPUT TYPE="hidden" name="TXNUUID" value="foo">
<INPUT TYPE="hidden" name="RDIR_URL" value=https://redirect.url/>
<INPUT TYPE="hidden" name="RDIR_TYPE" value="303">
<INPUT TYPE="hidden" name="GEP_MAC" value="Mxkskdhjsfhaiaskdsfj==">

<p><INPUT TYPE=submit VALUE="Submit"><p>
</form>
</body>
</html>
```

610

620

630

640

650

FIG. 6

700

Field	Description
TXNUUID	A Unique Transaction ID
RDIR_URL	The base redirection url (back to the ACS from HSM1).
RDIR_TYPE	Indicates the HTTP redirect type the HSM1 should return. The ACS will determine this value when initially receiving the PAReq by evaluating the UserAgent and HTTP version of the cardholder browser. The value will either be 302 or 303.
GEP_MAC	HMAC(k1,TXNUUID | RDIR_URL | RDIR_TYPE)

710 720 730 740

FIG. 7

800

Field	Description
EPIN1	The ISO 9564 Format-1 PINBLOCK encrypted under a key shared between HSM1 (front-end HSM) and HSM2 (the back-end HSM). This value shall be base64 encoded before being placed on the redirection URL.

810

FIG. 8

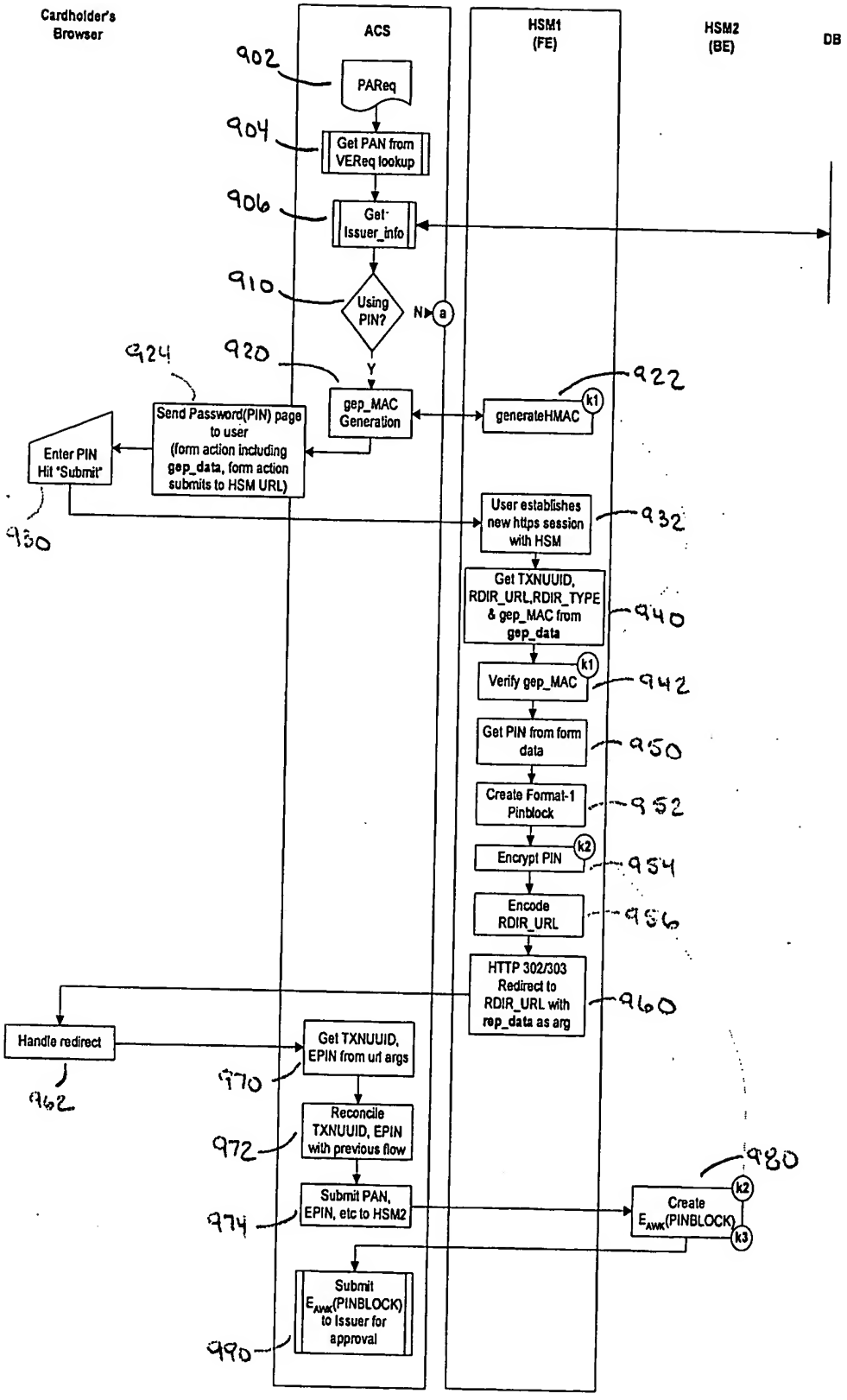
Cardholder's Browser
ACS
HSM1 (FE)
HSM2 (BE)
DB
902
PAReq
904
Get PAN from VEReq lookup
906
Get Issuer_info
910
Using PIN?
N
a
Y
924
920
Send Password(PIN) page to user (form action including gep_data, form action submits to HSM URL)
gep_MAC Generation
922
generateHMAC
k1
Enter PIN Hit "Submit"
930
User establishes new https session with HSM
932
Get TXNUUID, RDIR_URL,RDIR_TYPE & gep_MAC from gep_data
940
Verify gep_MAC
942
Get PIN from form data
950
Create Format-1 Pinblock
952
Encrypt PIN
k2
954
Encode RDIR_URL
956
HTTP 302/303 Redirect to RDIR_URL with rep_data as arg
960
Handle redirect
962
Get TXNUUID, EPIN from url args
970
Reconcile TXNUUID, EPIN with previous flow
972
Submit PAN, EPIN, etc to HSM2
974
980
Create E_{AWK}(PINBLOCK)
k3
Submit E_{AWK}(PINBLOCK) to Issuer for approval
990

FIG. 9

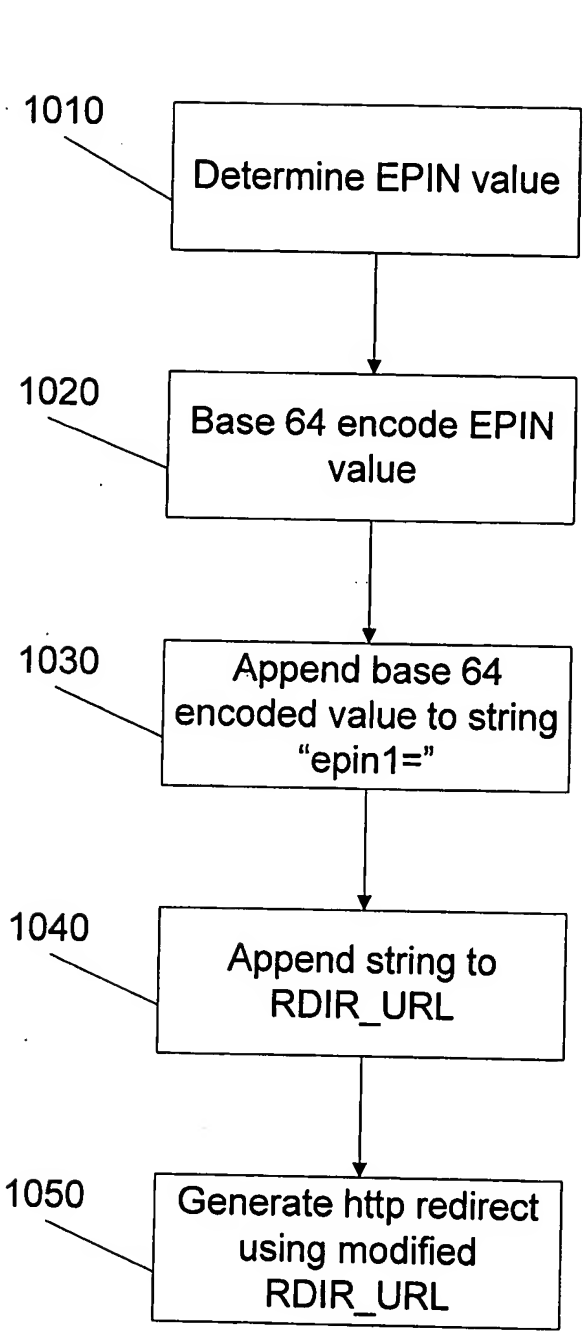
1000
1010
Determine EPIN value
1020
Base 64 encode EPIN value
1030
Append base 64 encoded value to string "epin1="
1040
Append string to RDIR_URL
1050
Generate http redirect using modified RDIR_URL

FIG. 10